CLAIMS

1. A security routing methodology comprising:

sensing information contained in an object;

analyzing said information to determine a security classification thereof; and

routing the object to at least one address selected at least partially in accordance with said security classification.

2. A security routing methodology according to claim 1 and wherein said object comprises a message.

3. A security routing methodology according to claim 1 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

4. A security routing methodology according to claim 1 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

5. A security routing methodology according to claim 1 and wherein said security classification comprises a secrecy classification.

6. A security routing methodology according to claim 1 and wherein said security classification comprises a danger classification.

7. A security routing methodology according to claim 1 and wherein said security

classification comprises a suspiciousness classification.

8. A security routing methodology according to claim 1 and wherein said security classification comprises a maliciousness classification.

9. A security routing methodology according to claim 1 and wherein analyzing said information comprises comparing said information against a security policy.

10. A security routing methodology according to claim 9 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

11. A security routing methodology according to claim 1 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

12. A security routing methodology according to claim 11 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

13. A security routing methodology according to claim 1 and wherein said object contains at least one at least one destination address.

14. A security routing methodology according to claim 13 and wherein said object comprises a message.

15. A security routing methodology according to claim 13 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

16. A security routing methodology according to claim 13 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

17. A security routing methodology according to claim 13 and wherein said at least one destination address is not one of said at least one address.

18. A security routing methodology according to claim 13 and wherein said at least one destination address is one of said at least one address.

19. A security routing methodology according to claim 13 and also comprising routing the object from said at least one address to said at least one destination address.

20. A security routing methodology according to claim 13 and also comprising routing the object from said at least one address directly to said at least one destination address.

21. A security routing methodology according to claim 13 and also comprising modifying the priority of said object.

22. A security routing methodology according to claim 13 and wherein said security classification comprises a secrecy classification.

23. A security routing methodology according to claim 22 and wherein said at least one destination address is not one of said at least one address.

24. A security routing methodology according to claim 22 and wherein said at least one destination address is one of said at least one address.

25. A security routing methodology according to claim 22 and also comprising routing the object from said at least one address to said at least one destination address.

26. A security routing methodology according to claim 22 and also comprising routing the object from said at least one address directly to said at least one destination address.

27. A security routing methodology according to claim 22 and also comprising modifying the priority of said object.

28. A security routing methodology according to claim 13 and wherein said security classification comprises a danger classification.

29. A security routing methodology according to claim 28 and wherein said at least one destination address is not one of said at least one address.

30. A security routing methodology according to claim 28 and wherein said at least one destination address is one of said at least one address.

31. A security routing methodology according to claim 28 and also comprising routing the object from said at least one address to said at least one destination address.

32. A security routing methodology according to claim 28 and also comprising routing the object from said at least one address directly to said at least one destination address.

33. A security routing methodology according to claim 28 and also comprising modifying the priority of said object.

34. A security routing methodology according to claim 13 and wherein said security classification comprises a suspiciousness classification.

35. A security routing methodology according to claim 34 and wherein said at least one destination address is not one of said at least one address.

36. A security routing methodology according to claim 34 and wherein said at least one destination address is one of said at least one address.

37. A security routing methodology according to claim 34 and also comprising routing the object from said at least one address to said at least one destination address.

38. A security routing methodology according to claim 34 and also comprising routing the object from said at least one address directly to said at least one destination address.

39. A security routing methodology according to claim 34 and also comprising modifying the priority of said object.

40. A security routing methodology according to claim 13 and wherein said security classification comprises a maliciousness classification.

41. A security routing methodology according to claim 40 and wherein said at least one destination address is not one of said at least one address.

42. A security routing methodology according to claim 40 and wherein said at least one destination address is one of said at least one address.

43. A security routing methodology according to claim 40 and also comprising routing the object from said at least one address to said at least one destination address.

44. A security routing methodology according to claim 40 and also comprising routing the object from said at least one address directly to said at least one destination address.

45. A security routing methodology according to claim 40 and also comprising modifying the priority of said object.

46. A security routing methodology according to claim 13 and wherein analyzing said information comprises comparing said information against a security policy.

47. A security routing methodology according to claim 46 and wherein said at least one destination address is not one of said at least one address.

48. A security routing methodology according to claim 47 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

49. A security routing methodology according to claim 46 and wherein said at least one destination address is one of said at least one address.

50. A security routing methodology according to claim 49 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

51. A security routing methodology according to claim 46 and also comprising routing the object from said at least one address to said at least one destination address.

52. A security routing methodology according to claim 51 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

53. A security routing methodology according to claim 46 and also comprising routing the object from said at least one address directly to said at least one destination address.

54. A security routing methodology according to claim 53 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

55. A security routing methodology according to claim 46 and also comprising modifying the priority of said object.

56. A security routing methodology according to claim 55 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

57. A security routing methodology according to claim 13 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

58. A security routing methodology according to claim 57 and wherein said at least one destination address is not one of said at least one address.

59. A security routing methodology according to claim 58 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

60. A security routing methodology according to claim 57 and wherein said at least one destination address is one of said at least one address.

61. A security routing methodology according to claim 60 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

62. A security routing methodology according to claim 57 and also comprising routing the object from said at least one address to said at least one destination address.

63. A security routing methodology according to claim 62 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and

suspiciousness classification.

64. A security routing methodology according to claim 57 and also comprising routing the object from said at least one address directly to said at least one destination address.

65. A security routing methodology according to claim 64 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

66. A security routing methodology according to claim 57 and also comprising modifying the priority of said object.

67. A security routing methodology according to claim 66 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

68. A security routing methodology comprising:

sensing information contained in an object directed to an address;

analyzing said information to determine a security classification thereof; and

routing the object to a selected at least one of a multiplicity of destinations enroute to said address in accordance with said security classification.

69. A security routing methodology according to claim 68 and wherein said object comprises a message.

70. A security routing methodology according to claim 68 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

71. A security routing methodology according to claim 68 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

72. A security routing methodology according to claim 68 and wherein said security classification comprises a secrecy classification.

73. A security routing methodology according to claim 68 and wherein said security classification comprises a danger classification.

74. A security routing methodology according to claim 68 and wherein said security classification comprises a suspiciousness classification.

75. A security routing methodology according to claim 68 and wherein said security classification comprises a maliciousness classification.

76. A security routing methodology according to claim 68 and wherein analyzing said information comprises comparing said information against a security policy.

77. A security routing methodology according to claim 76 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;
maliciousness classification; and
suspiciousness classification.

78. A security routing methodology according to claim 68 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

79. A security routing methodology according to claim 78 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

80. A security routing methodology comprising:

sensing information contained in an object;

analyzing said information to determine a security classification thereof; and

routing said object to at least one node selected from at least one destination node and at least one intermediate node which is selected at least partially in accordance with said security classification.

81. A security routing methodology according to claim 80 and wherein said object comprises a message.

82. A security routing methodology according to claim 80 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

83. A security routing methodology according to claim 80 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

84. A security routing methodology according to claim 80 and wherein said security classification comprises a secrecy classification.

85. A security routing methodology according to claim 80 and wherein said security classification comprises a danger classification.

86. A security routing methodology according to claim 80 and wherein said security classification comprises a suspiciousness classification.

87. A security routing methodology according to claim 80 and wherein said security classification comprises a maliciousness classification.

88. A security routing methodology according to claim 80 and wherein analyzing said information comprises comparing said information against a security policy.

89. A security routing methodology according to claim 88 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

90. A security routing methodology according to claim 80 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

91. A security routing methodology according to claim 90 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

92. A security routing methodology according to claim 80 and also comprising routing said message from said at least one selected node to at least one node addressed in said message.

93. A security routing methodology according to claim 92 and wherein said object comprises a message.

94. A security routing methodology according to claim 92 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

95. A security routing methodology according to claim 92 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

96. A security routing methodology according to claim 92 and wherein said security classification comprises a secrecy classification.

97. A security routing methodology according to claim 92 and wherein said security classification comprises a danger classification.

98. A security routing methodology according to claim 92 and wherein said security classification comprises a suspiciousness classification.

99. A security routing methodology according to claim 92 and wherein said security classification comprises a maliciousness classification.

100. A security routing methodology according to claim 92 and wherein analyzing said information comprises comparing said information against a security policy.

101. A security routing methodology according to claim 100 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

102. A security routing methodology according to claim 92 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

103. A security routing methodology according to claim 102 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

104. A security routing methodology comprising:

sensing, at a first node, information contained in an object;

analyzing, at said first node, said information to determine a security classification thereof; ands

routing said object to at least one node selected from at least one destination node and at least one intermediate node which is selected at least partially in accordance with said security classification.

105. A security routing methodology according to claim 104 and wherein said object comprises a message.

106. A security routing methodology according to claim 104 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

107. A security routing methodology according to claim 104 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

108. A security routing methodology according to claim 104 and wherein said security classification comprises a secrecy classification.

109. A security routing methodology according to claim 104 and wherein said security classification comprises a danger classification.

110. A security routing methodology according to claim 104 and wherein said security classification comprises a suspiciousness classification.

111. A security routing methodology according to claim 104 and wherein said security classification comprises a maliciousness classification.

112. A security routing methodology according to claim 104 and wherein analyzing said information comprises comparing said information against a security policy.

113. A security routing methodology according to claim 112 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

114. A security routing methodology according to claim 104 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

115. A security routing methodology according to claim 114 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

116. A system for routing an object comprising:

an object sensor, sensing information contained in an object;

an information analyzer, analyzing said information to determine a security classification thereof; and

a router, routing said object to at least one address selected at least partially in accordance with said security classification.

117. A system for routing an object according to claim 116 and wherein said object

comprises a message.

118. A system for routing an object according to claim 116 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

119. A system for routing an object according to claim 116 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

120. A system for routing an object according to claim 116 and wherein said security classification comprises a secrecy classification.

121. A system for routing an object according to claim 116 and wherein said security classification comprises a danger classification.

122. A system for routing an object according to claim 116 and wherein said security classification comprises a suspiciousness classification.

123. A system for routing an object according to claim 116 and wherein said security classification comprises a maliciousness classification.

124. A system for routing an object according to claim 116 and wherein analyzing said information comprises comparing said information against a security policy.

125. A system for routing an object according to claim 124 and wherein said

security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

126. A system for routing an object according to claim 116 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

127. A system for routing an object according to claim 126 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

128. A system for routing an object according to claim 116 and wherein said object contains at least one at least one destination address.

129. A system for routing an object according to claim 128 and wherein said object comprises a message.

130. A system for routing an object according to claim 128 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

131. A system for routing an object according to claim 128 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

132. A system for routing an object according to claim 128 and wherein said at least one destination address is not one of said at least one address.

133. A system for routing an object according to claim 128 and wherein said at least one destination address is one of said at least one address.

134. A system for routing an object according to claim 128 and also comprising routing the object from said at least one address to said at least one destination address.

135. A system for routing an object according to claim 128 and also comprising routing the object from said at least one address directly to said at least one destination address.

136. A system for routing an object according to claim 128 and also comprising modifying the priority of said object.

137. A system for routing an object according to claim 128 and wherein said security classification comprises a secrecy classification.

138. A system for routing an object according to claim 137 and wherein said at least one destination address is not one of said at least one address.

139. A system for routing an object according to claim 137 and wherein said at least one destination address is one of said at least one address.

140. A system for routing an object according to claim 137 and also comprising routing the object from said at least one address to said at least one destination address.

141. A system for routing an object according to claim 137 and also comprising routing the object from said at least one address directly to said at least one destination address.

142. A system for routing an object according to claim 137 and also comprising modifying the priority of said object.

143. A system for routing an object according to claim 128 and wherein said security classification comprises a danger classification.

144. A system for routing an object according to claim 143 and wherein said at least one destination address is not one of said at least one address.

145. A system for routing an object according to claim 143 and wherein said at least one destination address is one of said at least one address.

146. A system for routing an object according to claim 143 and also comprising routing the object from said at least one address to said at least one destination address.

147. A system for routing an object according to claim 143 and also comprising routing the object from said at least one address directly to said at least one destination address.

148. A system for routing an object according to claim 143 and also comprising modifying the priority of said object.

149. A system for routing an object according to claim 128 and wherein said security classification comprises a suspiciousness classification.

150. A system for routing an object according to claim 149 and wherein said at least one destination address is not one of said at least one address.

151. A system for routing an object according to claim 149 and wherein said at least one destination address is one of said at least one address.

152. A system for routing an object according to claim 149 and also comprising routing the object from said at least one address to said at least one destination address.

153. A system for routing an object according to claim 149 and also comprising routing the object from said at least one address directly to said at least one destination address.

154. A system for routing an object according to claim 149 and also comprising modifying the priority of said object.

155. A system for routing an object according to claim 128 and wherein said security classification comprises a maliciousness classification.

156. A system for routing an object according to claim 155 and wherein said at least one destination address is not one of said at least one address.

157. A system for routing an object according to claim 155 and wherein said at least one destination address is one of said at least one address.

158. A system for routing an object according to claim 155 and also comprising routing the object from said at least one address to said at least one destination address.

159. A system for routing an object according to claim 155 and also comprising routing the object from said at least one address directly to said at least one destination address.

160. A system for routing an object according to claim 155 and also comprising modifying the priority of said object.

161. A system for routing an object according to claim 128 and wherein analyzing said information comprises comparing said information against a security policy.

162. A system for routing an object according to claim 161 and wherein said at least one destination address is not one of said at least one address.

163. A system for routing an object according to claim 162 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

164. A system for routing an object according to claim 161 and wherein said at least one destination address is one of said at least one address.

165. A system for routing an object according to claim 164 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

166. A system for routing an object according to claim 161 and also comprising routing the object from said at least one address to said at least one destination address.

167. A system for routing an object according to claim 166 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and

suspiciousness classification.

168. A system for routing an object according to claim 161 and also comprising routing the object from said at least one address directly to said at least one destination address.

169. A system for routing an object according to claim 168 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

170. A system for routing an object according to claim 161 and also comprising modifying the priority of said object.

171. A system for routing an object according to claim 170 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

172. A system for routing an object according to claim 128 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

173. A system for routing an object according to claim 172 and wherein said at least one destination address is not one of said at least one address.

174. A system for routing an object according to claim 173 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

175. A system for routing an object according to claim 172 and wherein said at least one destination address is one of said at least one address.

176. A system for routing an object according to claim 175 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

177. A system for routing an object according to claim 172 and also comprising routing the object from said at least one address to said at least one destination address.

178. A system for routing an object according to claim 177 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

179. A system for routing an object according to claim 172 and also comprising routing the object from said at least one address directly to said at least one destination address.

180. A system for routing an object according to claim 179 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

181. A system for routing an object according to claim 172 and also comprising modifying the priority of said object.

182. A system for routing an object according to claim 181 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

183. A system for routing an object comprising:

an object sensor, sensing information contained in an object directed to an address;

an information analyzer, analyzing said information to determine a security classification thereof; and

a router, routing said object to a selected at least one of a multiplicity of destinations enroute to said address in accordance with said security classification.

184. A system for routing an object according to claim 183 and wherein said object comprises a message.

185. A system for routing an object according to claim 183 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

186. A system for routing an object according to claim 183 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

187. A system for routing an object according to claim 183 and wherein said security classification comprises a secrecy classification.

188. A system for routing an object according to claim 183 and wherein said security classification comprises a danger classification.

189. A system for routing an object according to claim 183 and wherein said security classification comprises a suspiciousness classification.

190. A system for routing an object according to claim 183 and wherein said security classification comprises a maliciousness classification.

191. A system for routing an object according to claim 183 and wherein analyzing said information comprises comparing said information against a security policy.

192. A system for routing an object according to claim 191 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

193. A system for routing an object according to claim 183 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

194. A system for routing an object according to claim 193 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

195. A system for routing an object comprising:

an object sensor, sensing information contained in an object;

an information analyzer, analyzing said information to determine a security classification thereof; and

a router, routing said object to at least one node selected from at least one destination node and at least one intermediate node which is selected at least partially in accordance with said security classification.

196. A system for routing an object according to claim 195 and wherein said object comprises a message.

197. A system for routing an object according to claim 195 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

198. A system for routing an object according to claim 195 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

199. A system for routing an object according to claim 195 and wherein said security classification comprises a secrecy classification.

200. A system for routing an object according to claim 195 and wherein said security classification comprises a danger classification.

201. A system for routing an object according to claim 195 and wherein said security classification comprises a suspiciousness classification.

202. A system for routing an object according to claim 195 and wherein said security classification comprises a maliciousness classification.

203. A system for routing an object according to claim 195 and wherein analyzing said information comprises comparing said information against a security policy.

204. A system for routing an object according to claim 203 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

205. A system for routing an object according to claim 195 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

206. A system for routing an object according to claim 205 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and

suspiciousness classification.

207. A system for routing an object according to claim 195 and also comprising routing said message from said at least one selected node to at least one node addressed in said message.

208. A system for routing an object according to claim 207 and wherein said object comprises a message.

209. A system for routing an object according to claim 207 and wherein said object comprises of at least one of:

a file:
an e-mail message;
a web page; and
a communication packet.

210. A system for routing an object according to claim 207 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

211. A system for routing an object according to claim 207 and wherein said security classification comprises a secrecy classification.

212. A system for routing an object according to claim 207 and wherein said security classification comprises a danger classification.

213. A system for routing an object according to claim 207 and wherein said security classification comprises a suspiciousness classification.

214. A system for routing an object according to claim 207 and wherein said security classification comprises a maliciousness classification.

215. A system for routing an object according to claim 207 and wherein analyzing said information comprises comparing said information against a security policy.

216. A system for routing an object according to claim 215 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

217. A system for routing an object according to claim 207 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

218. A system for routing an object according to claim 217 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

219. A system for routing an object comprising:

an object sensor, sensing information contained in an object;

an information analyzer, analyzing said information to determine a security classification thereof; and

a router, routing said object to at least one node selected from at least one destination node and at least one intermediate node which is selected at least partially in accordance with said security classification.

220. A system for routing an object according to claim 219 and wherein said object comprises a message.

221. A system for routing an object according to claim 219 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

222. A system for routing an object according to claim 219 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

223. A system for routing an object according to claim 219 and wherein said security classification comprises a secrecy classification.

224. A system for routing an object according to claim 219 and wherein said security classification comprises a danger classification.

225. A system for routing an object according to claim 219 and wherein said security classification comprises a suspiciousness classification.

226. A system for routing an object according to claim 219 and wherein said security classification comprises a maliciousness classification.

227. A system for routing an object according to claim 219 and wherein analyzing said information comprises comparing said information against a security policy.

228. A system for routing an object according to claim 227 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

229. A system for routing an object according to claim 219 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

230. A system for routing an object according to claim 229 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

231. A system for routing an object according to claim 116 and wherein said object sensor includes a network sniffer.

232. A system for routing an object according to claim 231 and wherein said object comprises a message.

233. A system for routing an object according to claim 231 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

234. A system for routing an object according to claim 231 and wherein information

contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

235. A system for routing an object according to claim 231 and wherein said security classification comprises a secrecy classification.

236. A system for routing an object according to claim 231 and wherein said security classification comprises a danger classification.

237. A system for routing an object according to claim 231 and wherein said security classification comprises a suspiciousness classification.

238. A system for routing an object according to claim 231 and wherein said security classification comprises a maliciousness classification.

239. A system for routing an object according to claim 231 and wherein analyzing said information comprises comparing said information against a security policy.

240. A system for routing an object according to claim 239 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

241. A system for routing an object according to claim 231 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

242. A system for routing an object according to claim 241 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;

maliciousness classification; and

suspiciousness classification.

243. A system for routing an object according to claim 231 and wherein said object contains at least one at least one destination address.

244. A system for routing an object according to claim 243 and wherein said object comprises a message.

245. A system for routing an object according to claim 243 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

246. A system for routing an object according to claim 243 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

247. A system for routing an object according to claim 243 and wherein said at least one destination address is not one of said at least one address.

248. A system for routing an object according to claim 247 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

249. A system for routing an object according to claim 243 and wherein said at least one destination address is one of said at least one address.

250. A system for routing an object according to claim 249 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

251. A system for routing an object according to claim 243 and also comprising routing the object from said at least one address to said at least one destination address.

252. A system for routing an object according to claim 251 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

253. A system for routing an object according to claim 243 and also comprising routing the object from said at least one address directly to said at least one destination address.

254. A system for routing an object according to claim 253 and wherein said security classification comprises at least one of:

secrecy classification;

danger classification;
maliciousness classification; and
suspiciousness classification.

255. A system for routing an object according to claim 243 and also comprising modifying the priority of said object.

256. A system for routing an object according to claim 255 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

257. A system for routing an object according to claim 243 and wherein analyzing said information comprises comparing said information against a security policy.

258. A system for routing an object according to claim 243 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

259. A system for routing an object according to claim 183 and wherein said object sensor includes a network sniffer.

260. A system for routing an object according to claim 259 and wherein said object comprises a message.

261. A system for routing an object according to claim 259 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and

a communication packet.

262. A system for routing an object according to claim 259 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

263. A system for routing an object according to claim 259 and wherein said security classification comprises a secrecy classification.

264. A system for routing an object according to claim 259 and wherein said security classification comprises a danger classification.

265. A system for routing an object according to claim 259 and wherein said security classification comprises a suspiciousness classification.

266. A system for routing an object according to claim 259 and wherein said security classification comprises a maliciousness classification.

267. A system for routing an object according to claim 259 and wherein analyzing said information comprises comparing said information against a security policy.

268. A system for routing an object according to claim 259 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

269. A system for routing an object according to claim 195 and wherein said object sensor includes a network sniffer.

270. A system for routing an object according to claim 269 and wherein said object

comprises a message.

271. A system for routing an object according to claim 269 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

272. A system for routing an object according to claim 269 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

273. A system for routing an object according to claim 269 and wherein said security classification comprises a secrecy classification.

274. A system for routing an object according to claim 269 and wherein said security classification comprises a danger classification.

275. A system for routing an object according to claim 269 and wherein said security classification comprises a suspiciousness classification.

276. A system for routing an object according to claim 269 and wherein said security classification comprises a maliciousness classification.

277. A system for routing an object according to claim 269 and wherein analyzing said information comprises comparing said information against a security policy.

278. A system for routing an object according to claim 269 and wherein analyzing

said information comprises comparing said information to an information contained in at least one other message.

279. A system for routing an object according to claim 207 and wherein said object sensor includes a network sniffer.

280. A system for routing an object according to claim 279 and wherein said object comprises a message.

281. A system for routing an object according to claim 279 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

282. A system for routing an object according to claim 279 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

283. A system for routing an object according to claim 279 and wherein said security classification comprises a secrecy classification.

284. A system for routing an object according to claim 279 and wherein said security classification comprises a danger classification.

285. A system for routing an object according to claim 279 and wherein said security classification comprises a suspiciousness classification.

286. A system for routing an object according to claim 279 and wherein said security classification comprises a maliciousness classification.

287. A system for routing an object according to claim 279 and wherein analyzing said information comprises comparing said information against a security policy.

288. A system for routing an object according to claim 279 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

289. A system for routing an object according to claim 219 and wherein said object sensor includes a network sniffer.

290. A system for routing an object according to claim 289 and wherein said object comprises a message.

291. A system for routing an object according to claim 289 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

292. A system for routing an object according to claim 289 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

293. A system for routing an object according to claim 289 and wherein said security classification comprises a secrecy classification.

294. A system for routing an object according to claim 289 and wherein said security classification comprises a danger classification.

295. A system for routing an object according to claim 289 and wherein said security classification comprises a suspiciousness classification.

296. A system for routing an object according to claim 289 and wherein said security classification comprises a maliciousness classification.

297. A system for routing an object according to claim 289 and wherein analyzing said information comprises comparing said information against a security policy.

298. A system for routing an object according to claim 289 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

299. A system for routing an object according to claim 116 also comprising:

a first interface providing interaction with said at least one first communication network; and

a second interface providing interaction with said at least one second communication network.

300. A system for routing an object according to claim 299 and wherein said object comprises a message.

301. A system for routing an object according to claim 299 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

302. A system for routing an object according to claim 299 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

303. A system for routing an object according to claim 299 and wherein said security classification comprises a secrecy classification.

304. A system for routing an object according to claim 299 and wherein said security classification comprises a danger classification.

305. A system for routing an object according to claim 299 and wherein said security classification comprises a suspiciousness classification.

306. A system for routing an object according to claim 299 and wherein said security classification comprises a maliciousness classification.

307. A system for routing an object according to claim 299 and wherein analyzing said information comprises comparing said information against a security policy.

308. A system for routing an object according to claim 307 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

309. A system for routing an object according to claim 299 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

310. A system for routing an object according to claim 309 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

311. A system for routing an object according to claim 299 and wherein said object contains at least one at least one destination address.

312. A system for routing an object according to claim 311 and wherein said object comprises a message.

313. A system for routing an object according to claim 311 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

314. A system for routing an object according to claim 311 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

315. A system for routing an object according to claim 311 and wherein said at least one destination address is not one of said at least one address.

316. A system for routing an object according to claim 315 and wherein said

security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

317. A system for routing an object according to claim 311 and wherein said at least one destination address is one of said at least one address.

318. A system for routing an object according to claim 317 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

319. A system for routing an object according to claim 311 and also comprising routing the object from said at least one address to said at least one destination address.

320. A system for routing an object according to claim 319 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

321. A system for routing an object according to claim 311 and also comprising routing the object from said at least one address directly to said at least one destination address.

322. A system for routing an object according to claim 321 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

323. A system for routing an object according to claim 311 and also comprising modifying the priority of said object.

324. A system for routing an object according to claim 323 and wherein said security classification comprises at least one of:
secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

325. A system for routing an object according to claim 311 and wherein analyzing said information comprises comparing said information against a security policy.

326. A system for routing an object according to claim 311 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

327. A system for routing an object according to claim 183 also comprising:

a first interface providing interaction with said at least one first communication network; and

a second interface providing interaction with said at least one second communication network.

328. A system for routing an object according to claim 327 and wherein said object comprises a message.

329. A system for routing an object according to claim 327 and wherein said object

comprises of at least one of:

a file:

an e-mail message;

a web page; and

a communication packet.

330. A system for routing an object according to claim 327 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

331. A system for routing an object according to claim 327 and wherein said security classification comprises a secrecy classification.

332. A system for routing an object according to claim 327 and wherein said security classification comprises a danger classification.

333. A system for routing an object according to claim 327 and wherein said security classification comprises a suspiciousness classification.

334. A system for routing an object according to claim 327 and wherein said security classification comprises a maliciousness classification.

335. A system for routing an object according to claim 327 and wherein analyzing said information comprises comparing said information against a security policy.

336. A system for routing an object according to claim 327 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

337. A system for routing an object according to claim 195 also comprising:

a first interface providing interaction with said at least one first communication network; and

a second interface providing interaction with said at least one second communication network.

338. A system for routing an object according to claim 337 and wherein said object comprises a message.

339. A system for routing an object according to claim 337 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

340. A system for routing an object according to claim 337 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

341. A system for routing an object according to claim 337 and wherein said security classification comprises a secrecy classification.

342. A system for routing an object according to claim 337 and wherein said security classification comprises a danger classification.

343. A system for routing an object according to claim 337 and wherein said security classification comprises a suspiciousness classification.

344. A system for routing an object according to claim 337 and wherein said security classification comprises a maliciousness classification.

345. A system for routing an object according to claim 337 and wherein analyzing said information comprises comparing said information against a security policy.

346. A system for routing an object according to claim 337 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

347. A system for routing an object according to claim 207 also comprising:

a first interface providing interaction with said at least one first communication network; and

a second interface providing interaction with said at least one second communication network.

348. A system for routing an object according to claim 347 and wherein said object comprises a message.

349. A system for routing an object according to claim 347 and wherein said object comprises of at least one of:

a file;
an e-mail message;
a web page; and
a communication packet.

350. A system for routing an object according to claim 347 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

351. A system for routing an object according to claim 347 and wherein said security classification comprises a secrecy classification.

352. A system for routing an object according to claim 347 and wherein said security classification comprises a danger classification.

353. A system for routing an object according to claim 347 and wherein said security classification comprises a suspiciousness classification.

354. A system for routing an object according to claim 347 and wherein said security classification comprises a maliciousness classification.

355. A system for routing an object according to claim 347 and wherein analyzing said information comprises comparing said information against a security policy.

356. A system for routing an object according to claim 347 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

357. A system for routing an object according to claim 219 also comprising:

a first interface providing interaction with said at least one first communication network; and

a second interface providing interaction with said at least one second communication network.

358. A system for routing an object according to claim 357 and wherein said object comprises a message.

359. A system for routing an object according to claim 357 and wherein said object comprises of at least one of:

a file;

an e-mail message;

a web page; and

a communication packet.

360. A system for routing an object according to claim 357 and wherein information contained in an object is selected from a set consisting of:

an object content;

an object header;

an object source; and

an object destination.

361. A system for routing an object according to claim 357 and wherein said security classification comprises a secrecy classification.

362. A system for routing an object according to claim 357 and wherein said security classification comprises a danger classification.

363. A system for routing an object according to claim 357 and wherein said security classification comprises a suspiciousness classification.

364. A system for routing an object according to claim 357 and wherein said security classification comprises a maliciousness classification.

365. A system for routing an object according to claim 357 and wherein analyzing said information comprises comparing said information against a security policy.

366. A system for routing an object according to claim 357 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.

367. A system for routing an object according to claim 128 and wherein address of said system is at least one of said at least one destination address.

368. A system for routing an object according to claim 367 and wherein said object comprises a message.

369. A system for routing an object according to claim 367 and wherein said object comprises of at least one of:

a file:
an e-mail message;
a web page; and
a communication packet.

370. A system for routing an object according to claim 367 and wherein information contained in an object is selected from a set consisting of:

an object content;
an object header;
an object source; and
an object destination.

371. A system for routing an object according to claim 367 and wherein said at least one destination address is not one of said at least one address.

372. A system for routing an object according to claim 371 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

373. A system for routing an object according to claim 367 and wherein said at least one destination address is one of said at least one address.

374. A system for routing an object according to claim 373 and wherein said

security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

375. A system for routing an object according to claim 367 and also comprising routing the object from said at least one address to said at least one destination address.

376. A system for routing an object according to claim 375 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

377. A system for routing an object according to claim 367 and also comprising routing the object from said at least one address directly to said at least one destination address.

378. A system for routing an object according to claim 377 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

379. A system for routing an object according to claim 367 and also comprising modifying the priority of said object.

380. A system for routing an object according to claim 379 and wherein said security classification comprises at least one of:

secrecy classification;
danger classification;
maliciousness classification; and
suspiciousness classification.

381. A system for routing an object according to claim 367 and wherein analyzing said information comprises comparing said information against a security policy.

382. A system for routing an object according to claim 367 and wherein analyzing said information comprises comparing said information to an information contained in at least one other message.